TECHNOLOGY DRIVEN. WARFIGHTER FOCUSED.

TARDEC Certification & Accreditation of IT Software for Tactical Systems Issues

October 16, 2007

- **Introduction**
- **What is DIACAP**
- **Why DIACAP**
- **Army C&A process**
- **Agent of the Certification Authority**
- **IA Requirement for Tactical Systems**
- **Deployment of Secure Software in Tactical Vehicles**
- **Questions**

What is DIACAP?

- **DoD Information Assurance Certification and Accreditation Process (DIACAP)**
- **A dynamic Information Assurance (IA) certification and accreditation (C&A) process that supports the net-centric, Global Information Grid (GIG) - based environment**

Why DIACAP

- Satisfies need for a dynamic certification and accreditation (C&A) process for the Global Information Grid (GIG)
- Net-centric applications which cannot be met with the current C&A methodology
- Replaces "DoD Information Technology Security C&A Process (DITSCAP)"
- Provides new focus on STANDARDIZED Controls
- Is consistent with Title III of the E-Government Act, Federal Information Security Management Act (FISMA), and DoD Directive 8500.1 and DoDI 8500.2

Army C&A Process

- Issues
  - Software Developer (system Owner) limited knowledge of the C&A process, e.g.
    - Selects an ACA
    - Request IACORA for Certification Accreditation Representative (CAR)
    - Submits the System Information Profile (SIP)
    - Create Artifacts to support IA controls
    - Schedule ACA for pre-assessment/assessment
    - Create a Plan of Action and Milestone (POAM) to mitigate vulnerabilities

Army C&A Process Cont.

- ACAs
  - 6 ACAs to support Army C&A efforts (TACOM becoming an ACA in progress)
  - Few ACAs are experience with C&A of Tactical Software System (CECOM, ARL/SLAD, …)

- IACORA Office
  - Limited Staff
  - Limited knowledge and experience with C&A of tactical software

Agent of the Certification Authority (ACA) Validation and Verification process

- **Issues with ACA Validation and Verification process:**
  - **Limited number of ACAs**
    - **6 ACAs to support Army C&A efforts (TACOM becoming an ACA in progress)**
  - **Lack of STIGs applying specifically to Tactical System**
  - **Lack of Tactical Labs**
  - **IA controls developed mostly with Business Systems in mind**
  - **Input from PEOs that ACA certification guidance are different**
    - **IACORA should establish and promote standardized guidance for interpretation of IA requirements.**

IA Requirement for Tactical Systems

- **Issues with IA Requirements for Tactical Systems software:**
  - **Contractor develop software components with no IA responsibilities specified in development contract**
    - **Cost of Malicious Code Review (MCA)**
    - **Trained ACAs who can perform MCA limited**
    - **Increase cost to perform MCA**
  - **Specific COTS/GOTS developed software product**
    - **NIAP approval list**
    - **Army software approval list**

Deployment of Secure Software in Tactical Vehicles

- **Issues with Deployed software systems:**
  - **Applying IA Controls to tactical weapon systems**
    - **Encryption**
    - **Classification of Information**
    - **Tactical System Requirements**
    - **Applying Critical IAVA**
  - **Maintaining certified and accredited software configuration in deployed software**
    - **No software engineers deployed**
    - **Software labs**
    - **No standard operating procedures (SOPs)**
    - **No IA/IT training for Software Developer**

Summary

- What is DIACAP - DoD/Army process of accrediting and certifying all IS within its inventory throughout their lifecycle

- Why DIACAP – to comply FISMA guidelines

- Agent of the Certification Authority – independent validator for the Army CA, limited knowledge of software development and how to comply with DIACAP

- IA Requirement for Tactical Systems – No firm guidelines on how to comply with AR 25-2.

- Deployment of Secure Software in Tactical Vehicles- Limited IA personnel or tools available

TARDEC Point of Contacts

- **TARDEC Next Gen Software Engineering Center - IA Support**
  - **Mr. Marion Williams – 586–574-6963, Marion.Williams2@us.army.mil**
  - **Mr. Jeffrey Wong – 586-753-2273, Jeffrey.Wong@us.army.mil**
  - **Mr. Jimmie Walker – 586-574-5034, Jimmie.Walker@us.army.mil**

Questions

Backup slides

DIACAP Frequently Asked Questions

- **Who do I contact with questions on the Interim DIACAP Instruction, KS?**
  - **The DIACAP Program Technical Inquiries Team can be reached by web, email or phone:**
  - **Phone: (703)377-0001**
    email: support@diacap-knowledgeservice.org
  - **Web: Help and Feedback Link in Knowledge Service**
  - **Hours of operation: 0900-1700 EST, Monday – Friday**

DIACAP Frequently Asked Questions

- **How will the signature of the DIACAP affect programs that already have a mature DITSCAP package?**
  - **DoDI 8510 provides a detailed Timeline and Instruction that addresses various scenarios, i.e., an unaccredited or new start Information System (IS), an IS with a DITSCAP ATO, an IS with a partially complete SSAA, with or without implementation of DoDI 8500.2 IA Controls etc. The Timelines provide detailed instructions for transitioning to the DIACAP within the directed timeframe. The timelines can be found in the Transitioning to DIACAP section in the Knowledge Service.**

DIACAP Frequently Asked Questions

- **Does the DIACAP supersede DITSCAP?**
  - **Yes. The DoD is changing the way it acquires, operates and uses IT in conjunction with federal requirements and guidelines. DITSCAP is a system-based, paper-oriented process that assumes minimal connectivity and was not designed to operate in a dynamic IT environment.**

UNCLASSIFIED

DIACAP Frequently Asked Questions

- **Does a system have to implement those IA Controls that are particular to the system within the testing environment, or just the technical controls that would actually transfer when the system is sent into the field?**
  - **The system is fully tested within the test environment and the full ATO package (all IA Controls based on the MAC and CL of the system) is sent to the field with the system. When the system is installed in the field, the field organization would determine the MAC and CL of the system within their environment, review the accompanying ATO package, determine which IA Controls were implemented during development that are still valid (meaning they are required under the MAC and CL the field organization has determined), and which that must be newly implemented.**

DIACAP Frequently Asked Questions

- **What content is in the Knowledge Service and will it be immediately available to the IA community when the Instruction is signed?**
  - **The Knowledge Service will provide supplementary guidance supporting implementation material for IA Controls, templates, diagrams and figures, as well as tools and functionality to support collaboration. This content is not intended to be directive in nature, but is established as a baseline with the anticipation that the DoD components will come forward to provide additional guidance and specificity on the existing content. The Knowledge Service will be available upon signature of the Instruction.**

DIACAP Frequently Asked Questions

- **When will training be available to the Services and what is the training mechanism?**
  - **DISA is setting up a program that is expected to include classroom training as well as CBT and distance learning as they have done with DITSCAP previously. A primary source of information and guidance is the DIACAP Knowledge Service which will be a ready source of DIACAP Implementation Guidance for the community at all levels.**